Claims

I claim:

1. A method for secure electronic transaction authentication, comprising the steps of:

   a. obtaining transaction information from a vendor;

   b. obtaining user information, including a secret key from a user;

   c. electronically performing a message authentication code ("MAC") function on at least some of the transaction information and some of the user information; and

   d. using a result of the MAC function as private transaction information.

2. The method of claim 1, wherein the step of obtaining transaction information comprises obtaining at least one of a name of the vendor, a URL, a transaction amount, a date of transaction, and a time of transaction.

3. The method of claim 1, further comprising the step of adding a counter value to the transaction information.

4. The method of claim 1, wherein the step of using the result of the MAC function comprises using the result as at least a part of a credit card number.

5. The method of claim 1, wherein the step of using the result of the MAC function as private transaction information comprises using the result as at least a part of a user's name.

6. A method for verifying secure information for a user, where the user has a secret key, comprising the steps of:

   a. receiving the secure information;

   b. receiving transaction information;

   c. receiving user information;

   d. electronically performing a message authentication code ("MAC") function on at least some of the transaction information and at least some of the user information using the secret key;

   e. comparing a result of the MAC function with the

received secure information; and

f. verifying the received secure information if the result of the MAC function is identical to the received secure information.

7. The method of claim 6, wherein the step of receiving the secure information comprises receiving from a vendor private transaction information at least partially containing the result of the MAC function.

8. The method of claim 7, wherein the step of receiving from a vendor private transaction information further comprises receiving a user's name at least partially containing the results of the MAC function.

9. The method of claim 7, wherein the step of receiving from a vendor private transaction information further comprises receiving a credit card number at least partially containing the results of the MAC function.

10. The method of claim 6, wherein the step of receiving transaction information comprises receiving at least one of a name of the vendor, a URL, a transaction amount, a date of transaction, a time of transaction, a name of an item purchased, or an invoice number.

11. A method for conducting a secure electronic transaction, comprising the steps of:

a. obtaining transaction information from a vendor;

b. obtaining user information, including a secret key;

c. processing secure information by electronically performing a first MAC function on at least some of the transaction information and some of the user information using the secret key;

d. using the secure information in private transaction information;

e. a verifier receiving the secure information;

f. the verifier receiving the transaction information;

g. the verifier receiving the user information;

h. electronically performing a second MAC function on at least some of the transaction information and at least some of the user information using the secret key;

i. comparing a result of the second MAC function with the received secure information; and

j. verifying the received secure information if the result of the second MAC function are identical to the received secure information.

12. The method of claim 11, wherein the step of obtaining transaction information comprises obtaining at least one of a name of the vendor, a URL, a transaction amount, a date of transaction, a time of transaction, a name of an item purchased, or an invoice number.

13. The method of claim 11, wherein the step of using the secure information comprises using the result as at least a part of a credit card number.

14. The method of claim 11, wherein the step of using the secure information comprises using the result as at least a part of a user's name.

15. The method of claim 11, wherein the step of receiving the secure information comprises receiving from a vendor a credit card number at least partially containing the results of the first MAC function.

16. The method of claim 11, wherein the step of receiving the secure information comprises receiving from the vendor a user's name at least partially containing the result of the first MAC function.

17. The method of claim 11, comprising the step of further adding a counter value to the transaction information.

18. An apparatus for providing secure electronic transaction authentication comprising:

a. an input configured to obtain transaction information from a vendor, and user information from a user, including a user's secret key;

b. a processor configured to receive the transaction information and the user information and to electronically perform a MAC function on at least some of the transaction information and some of the user information using the secret key; and

c. an output configured to output a result of the MAC function for use as private

transaction information.

19. The apparatus of claim 18, wherein the transaction information comprises at least one of a name of the vendor, a URL, a transaction amount, a date of transaction, and a time of transaction.

20. The apparatus of claim 18, wherein the processor is further configured to add a counter value to the transaction information.

21. The apparatus of claim 18, wherein the private transaction information comprises at least part of a credit card number.

22. The apparatus of claim 18, wherein the private transaction information comprises at least part of a user's name.

23. An apparatus for verifying secure information for a user, where the user has a secret key, comprising:

a. an input configured to receive the secure information, transaction information, and user information;

b. a processor configured to obtain the transaction information and the user information and to electronically perform a MAC function on at least some of the transaction information and at least some of the user information using the secret key;

c. the processor further configured to obtain the secure information and a result of the MAC function, and to compare the result of the MAC function with the received secure information; and

d. an output configured to output a verification of the secure information if the result of the MAC function are identical to the received secure information.

24. The apparatus of claim 23, wherein the private transaction information is a credit card number at least partially containing the secure information.

25. The apparatus of claim 23, wherein the private transaction information is a user's name at least partially containing the secure information.

26. The apparatus of claim 23, wherein the step of receiving transaction information

comprises receiving at least one of a name of the vendor, a URL, a transaction amount, a date of transaction, a time of transaction, a name of an item purchased, and an invoice number.

27. An apparatus for conducting a secure electronic transaction, comprised of:

a. an input for receiving transaction information from a vendor, and for obtaining user information from the user, including a secret key;

c. a first processor configured to receive the transaction information and the user information and to process secure information by performing a first MAC function on at least some of the transaction information and some of the user information using the secret key;

d. an output configured to output the secure information for use in the secure electronic transaction;

e. a verifier input for receiving the secure information, the transaction information, and the user information;

f. a second processor configured to receive the transaction information and the user information, and to perform a second MAC function on at least some of the transaction information and at least some of the user information, and to compare a result of the second MAC function with the received secure information; and

g. an output configured to output a verification of the secure information if the result of the second MAC function are identical to the received secure information.

29. The apparatus of claim 27, wherein the transaction information is at least one of a name of the vendor, a URL, a transaction amount, a date of transaction, a time of transaction, a name of an item purchased, and an invoice number.

30. The apparatus of claim 27, wherein the secure information is used as at least a part of a credit card number.

31. The apparatus of claim 27, wherein the secure information is used as at least a part of a user's name.

32. The apparatus of claim 27, wherein the secure information is a credit card number at least partially containing the result of the first MAC function.

33. The apparatus of claim 27, wherein the secure information is a user's name at least partially containing the result of the first MAC function.

34. The apparatus of claim 27, wherein the processor for performing the first MAC function adds a counter value to the transaction information.